SIEMENS

Using virus scanners 1

Configuration 2

SIMATIC

Process Control System PCS 7 McAfee VirusScan (V8.5; V8.5i; V8.7) Configuration

Commissioning Manual

08/2009
A5E02634985-01

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION

with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken.

CAUTION

without a safety alert symbol, indicates that property damage can result if proper precautions are not taken.

NOTICE

indicates that an unintended result or situation can occur if the corresponding information is not taken into account.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation for the specific task, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be adhered to. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of the Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E02634985-01
℗ 08/2009

Copyright © Siemens AG 2009.
Technical data subject to change

Table of contents

1 Using virus scanners 5

1.1 Preface 5

1.2 Using virus scanners 6
1.2.1 Introduction 6
1.2.2 Definitions and information 6
1.2.3 Principle structure of the virus scanner architecture 7
1.2.4 Using antivirus software 8

2 Configuration 9

2.1 Introduction 9

2.2 Configuration of the policies 9

2.3 Central settings 10
2.3.1 "Settings" tab 10
2.3.2 Tasks in process mode 10
2.3.3 Deploying virus definition files 11
2.3.4 Checking the deployment of the virus definition files 13

2.4 On-Access General Policies 14
2.4.1 "General" tab 14
2.4.2 "ScriptScan" tab 15
2.4.3 "Blocking" tab 16
2.4.4 "Messages" tab 17

2.5 On-Access Default Processes Policies 18
2.5.1 "Detection" tab 18
2.5.2 "Advanced" tab 19
2.5.3 "Actions" tab 20
2.5.4 "Unwanted Programs" tab 21

2.6 On-Access Low-Risk Processes Policies 22

2.7 On-Access High-Risk Processes Policies 22

2.8 On Delivery E-Mail Scan Policies Policies 22

2.9 User Interface Policies 23
2.9.1 "Display Options" tab 23
2.9.2 "Password Options" tab 24

2.10 Warning guidelines 24

2.11 Access Protection Policies 25

2.12 Buffer overflow protection policies 25

2.13 Unwanted Programs Policies 25

2.14 Quarantine Manager Policies 25

1 Using virus scanners

1.1 Preface

Important information about this whitepaper

The compatibility of the virus scanners recommended for PCS 7 and WinCC has been tested with the systems. The recommended settings for these virus scanners have been chosen to ensure the reliable real time operation of PCS 7 is not adversely affected by the virus scanner software.

These recommendations describe how to discover and make effective as comprehensively as possible the currently known, best possible compromise between the target, virus and damage software, and ensure an as determinable as possible time response of the PCS 7 control system can be achieved in all operating phases.

If you choose different settings for the virus scanner, this could have negative effects on the real-time behavior.

Purpose of this documentation

This documentation describes the recommended settings for virus scanner software in combination with PCS 7 and WinCC following the virus scanner installation.

Required knowledge

This documentation is aimed at anyone who is involved in configuring, commissioning and operating automated systems based on SIMATIC PCS 7 or WinCC. Knowledge of administration and IT techniques for Microsoft Windows operating systems is assumed.

Validity of the documentation

The documentation applies to process control systems equipped with the respective product version of PCS 7 or WinCC.

NOTICE
Note that certain virus scanners are only approved for certain product versions. Additional information is available in the Internet at the following address: http://support.automation.siemens.com/ (http://support.automation.siemens.com/WW/view/en/10154608)

1.2 Using virus scanners

1.2.1 Introduction

Using virus scanners in a process control system is only effective when they are part of a comprehensive security concept. A virus scanner alone cannot protect a process control system against hostile attacks.

The security concept PCS 7 / WinCC is available on the Internet under:

http://support.automation.siemens.com (http://support.automation.siemens.com)

Virus scanners should comply with the requirements described in the security concepts of PCS 7 / WinCC.

1.2.2 Definitions and information

Basic principle

The use of a virus scanner should never inhibit a plant in runtime.

Virus scanners

A virus scanner is a software that detects, blocks or eliminates harmful program routines (computer viruses, worms, etc.).

Scan engine (scanner module)

The scan engine is a component of the virus scanner software that can examine data for harmful software.

Virus signature file (virus pattern file or virus definition file)

This file provides the virus signatures to the scan engine, which uses it to search through data for harmful software.

Virus scan client

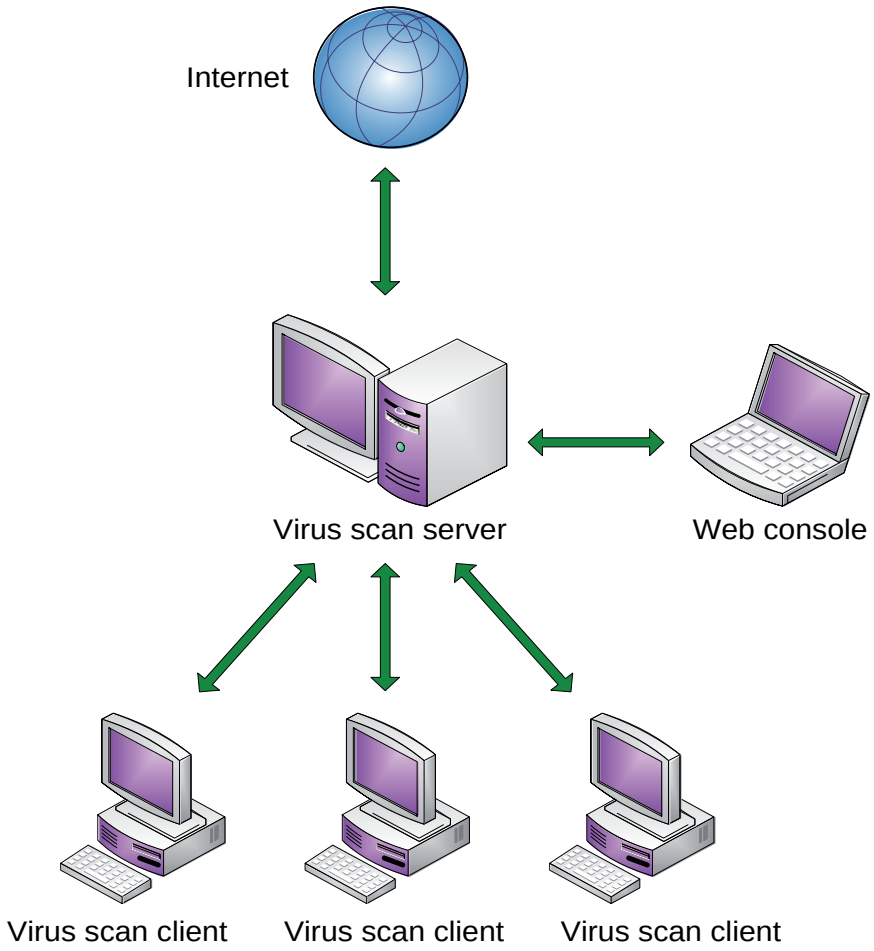
The virus scan client is a computer which is examined for viruses and managed by the virus server.

Virus scan server

The virus scan server is a computer which centrally manages virus scan clients, loads virus signature files and deploys them on the virus scan clients.

1.2.3 Principle structure of the virus scanner architecture

A virus scan server receives its virus signatures from the update server of the respective virus scan manufacturer in the Internet or from an upstream virus scan server and manages its virus scan clients.
Remote access to the virus scan server is available via web console.



1.2.4 Using antivirus software

Information for configuration of local virus scanners

- **Integrated firewall of the virus scanner**
  The local Windows firewall is used as of PCS 7 V7.0 and configured with the SIMATIC Security Control (SSC) component. The firewalls integrated in the virus scanners are therefore not installed.
- **Manual scan (manual scan, on demand scan)**
  A manual scan should never be performed on virus scan clients during process mode (runtime). This should take place at regular intervals, e.g. during maintenance, on all computers of the system.
- **Automatic scan (auto-protect, on-access scanning)**
  With automatic scanning, it is sufficient to check the incoming data traffic.
- **Scheduled scan (planned search, on demand scan)**
  A scheduled scan should never be performed on virus scan clients during process mode (runtime).
- **Displaying messages**
  To ensure that process mode is not inhibited, no messages should be displayed on the virus scan clients.
- **Drives**
  To avoid overlapping scanning of network drives, only local drives are scanned.
- **E-mail scan**
  Scanning of e-mail can be disabled except on the engineering station which receives e-mails.
- **Division into groups**
  Organize your virus scan clients in groups.
- **Deployment of the virus signature (pattern update)**
  The deployment of the virus signatures to the virus scan clients is performed by the upstream virus scan server. Test the virus signatures in a test system before deploying them in process mode to ensure that work correctly. Distribute the virus signatures manually to the respective groups.
- **Update the virus scan engine**
  Do not conduct the virus scan engine update in runtime as these updates will probably require you to restart the virus scan client.

Note on installation

The software installation must be carried out from a virus-free storage location (e.g. from a file server with its own virus scanner or from a certified DVD). During the software installation, automatic changes are often carried out in the operating system. An enabled virus scanner must not obstruct or falsify the software installation.

Configuration 2

2.1 Introduction

Only selected versions of the "McAfee VirusScan" Corporate Edition virus scanner have been approved for some versions of PCS 7. The settings described below that have changed in comparison to the standard version were tested for PCS7.

Approved virus scanners for the following PCS 7 versions

You can find the latest overview of the virus scanners authorized for a PCS 7 version at the following Internet address:
http://support.automation.siemens.com (http://support.automation.siemens.com/WW/view/en/10154608)

2.2 Configuration of the policies

All settings listed for the "Workstation" must also always be made for the "Server".

2.3 Central settings

2.3.1 "Settings" tab

"Enable global updating" setting; "No" button: **Enabled**

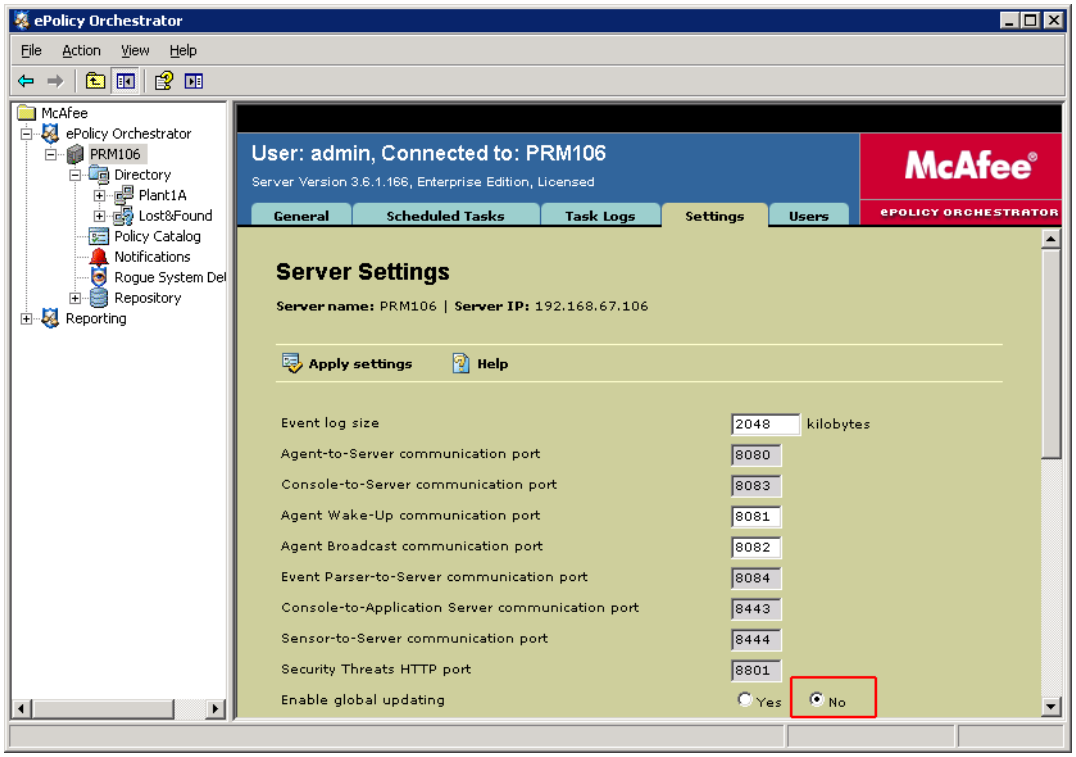


Figure 2-1 "ePolicy Orchestrator" dialog box, "Server Settings" tab

2.3.2 Tasks in process mode

The following tasks were not affected in process mode:

Task type	Software	Parameters	Purpose
Agent reactivation	ePolicy Orchestrator Agent		Prompts agent in a virus scan client to contact ePolicy Orchestrator server.
Updating	ePolicy Orchestrator Agent	DAT, Extra.DAT, SuperDAT	Updating virus signature files

2.3.3 Deploying virus definition files

Task and schedule settings

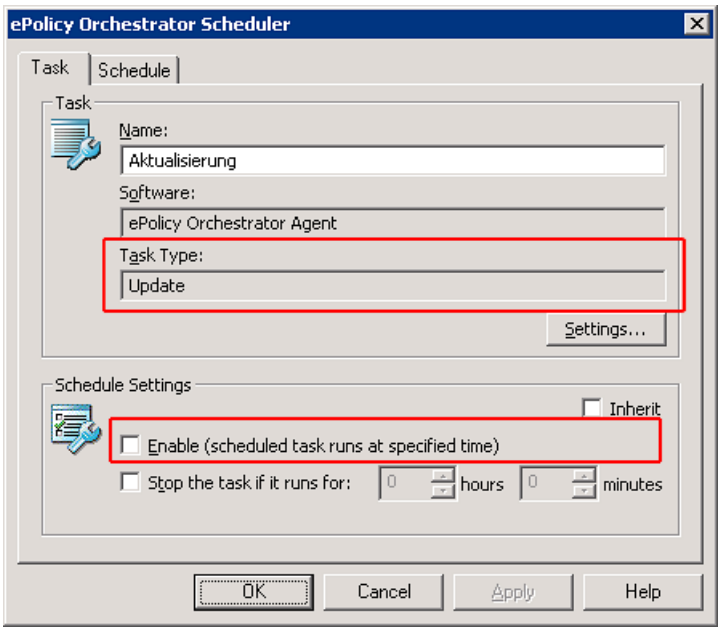


Figure 2-2 "ePolicy orchestrator planner" dialog box, "Task" tab

Ensure that "update" task type is selected for the update task. Only if the virus definition files are to be deployed should you activate the check box "Activate (planned task will be carried out at a specified time").
The virus scan client updates the virus definition files in accordance with the planning settings if it has transferred the amended guideline.

- In the drop-down list "Schedule task" select the "Run Immediately" setting.

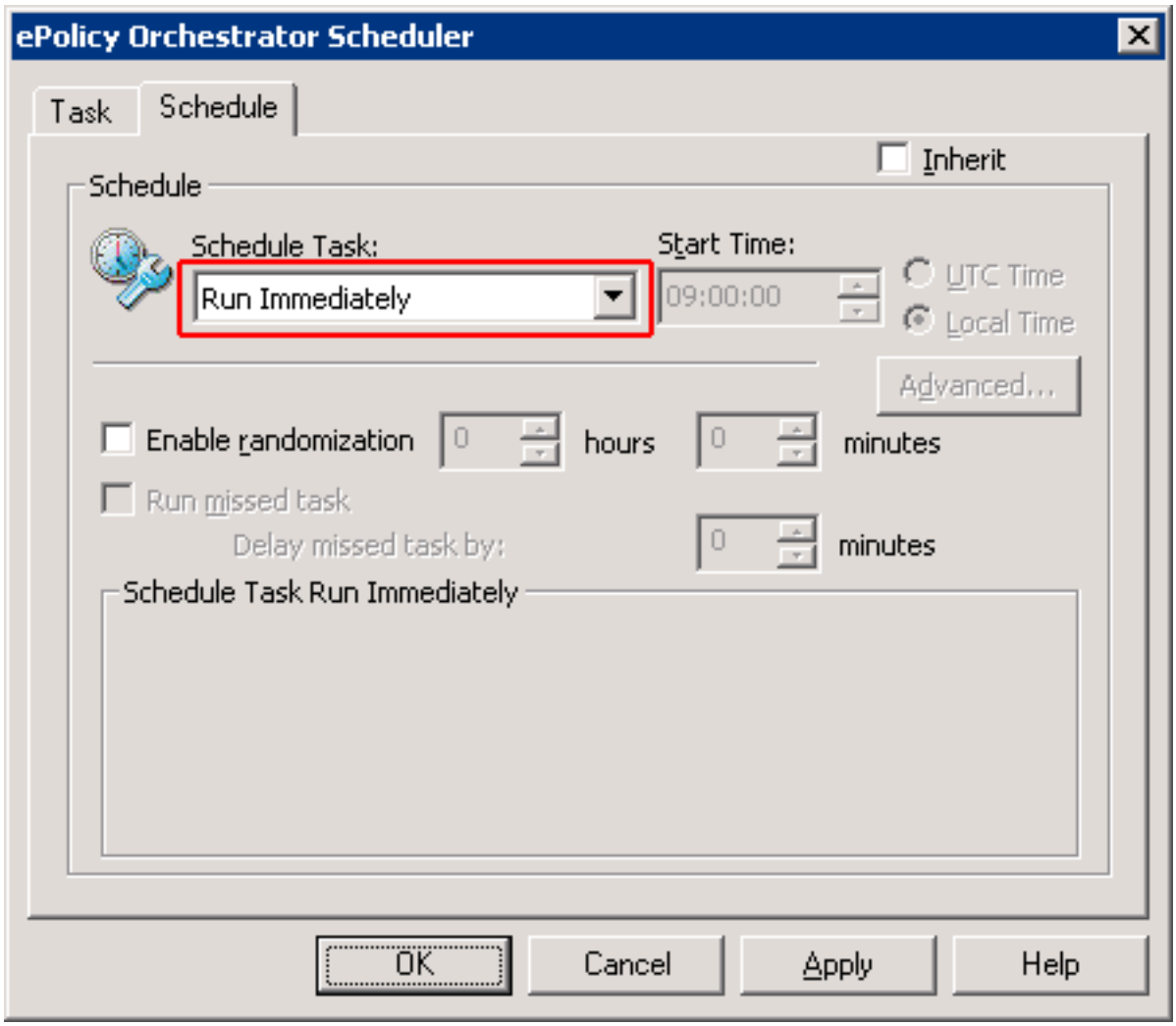


Figure 2-3 "ePolicy orchestrator planner" dialog box, "Plan" tab

2.3.4 Checking the deployment of the virus definition files

You will find the overview in the tree structure **McAffee > Reporting > ePO Databases> <Database name> > Requests > Events > All Product Update Events**.

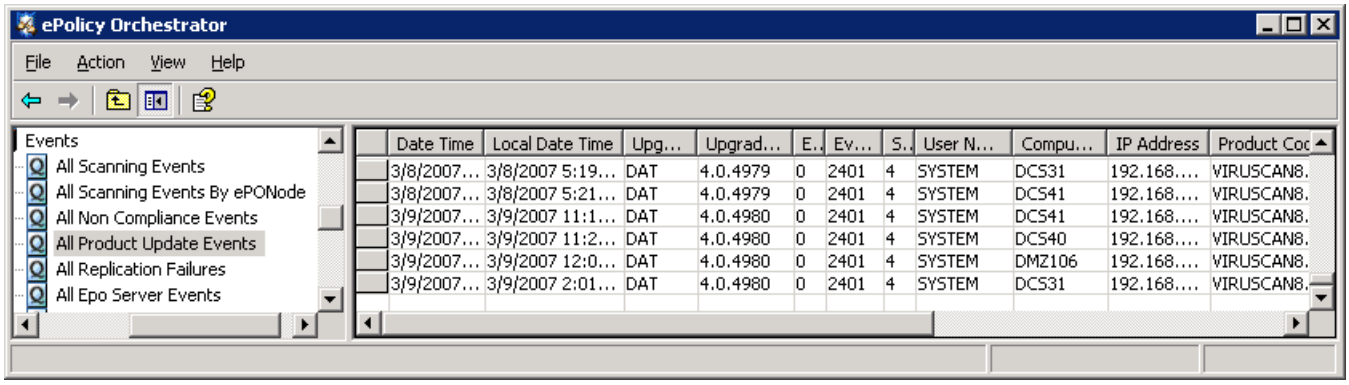

ePolicy Orchestrator
File Action View Help
Events
All Scanning Events
All Scanning Events By ePONode
All Non Compliance Events
All Product Update Events
All Replication Failures
All Epo Server Events
Date Time | Local Date Time | Upg... | Upgrad... | E.. | Ev... | S.. | User N... | Compu... | IP Address | Product Coc
3/8/2007... | 3/8/2007 5:19... | DAT | 4.0.4979 | 0 | 2401 | 4 | SYSTEM | DCS31 | 192.168.... | VIRUSCAN8.
3/8/2007... | 3/8/2007 5:21... | DAT | 4.0.4979 | 0 | 2401 | 4 | SYSTEM | DCS41 | 192.168.... | VIRUSCAN8.
3/9/2007... | 3/9/2007 11:1... | DAT | 4.0.4980 | 0 | 2401 | 4 | SYSTEM | DCS41 | 192.168.... | VIRUSCAN8.
3/9/2007... | 3/9/2007 11:2... | DAT | 4.0.4980 | 0 | 2401 | 4 | SYSTEM | DCS40 | 192.168.... | VIRUSCAN8.
3/9/2007... | 3/9/2007 12:0... | DAT | 4.0.4980 | 0 | 2401 | 4 | SYSTEM | DMZ106 | 192.168.... | VIRUSCAN8.
3/9/2007... | 3/9/2007 2:01... | DAT | 4.0.4980 | 0 | 2401 | 4 | SYSTEM | DCS31 | 192.168.... | VIRUSCAN8.

Figure 2-4 Checking the deployment of the virus definition files

2.4 On-Access General Policies

2.4.1 "General" tab

"Floppy during shutdown" check box: **Disabled**

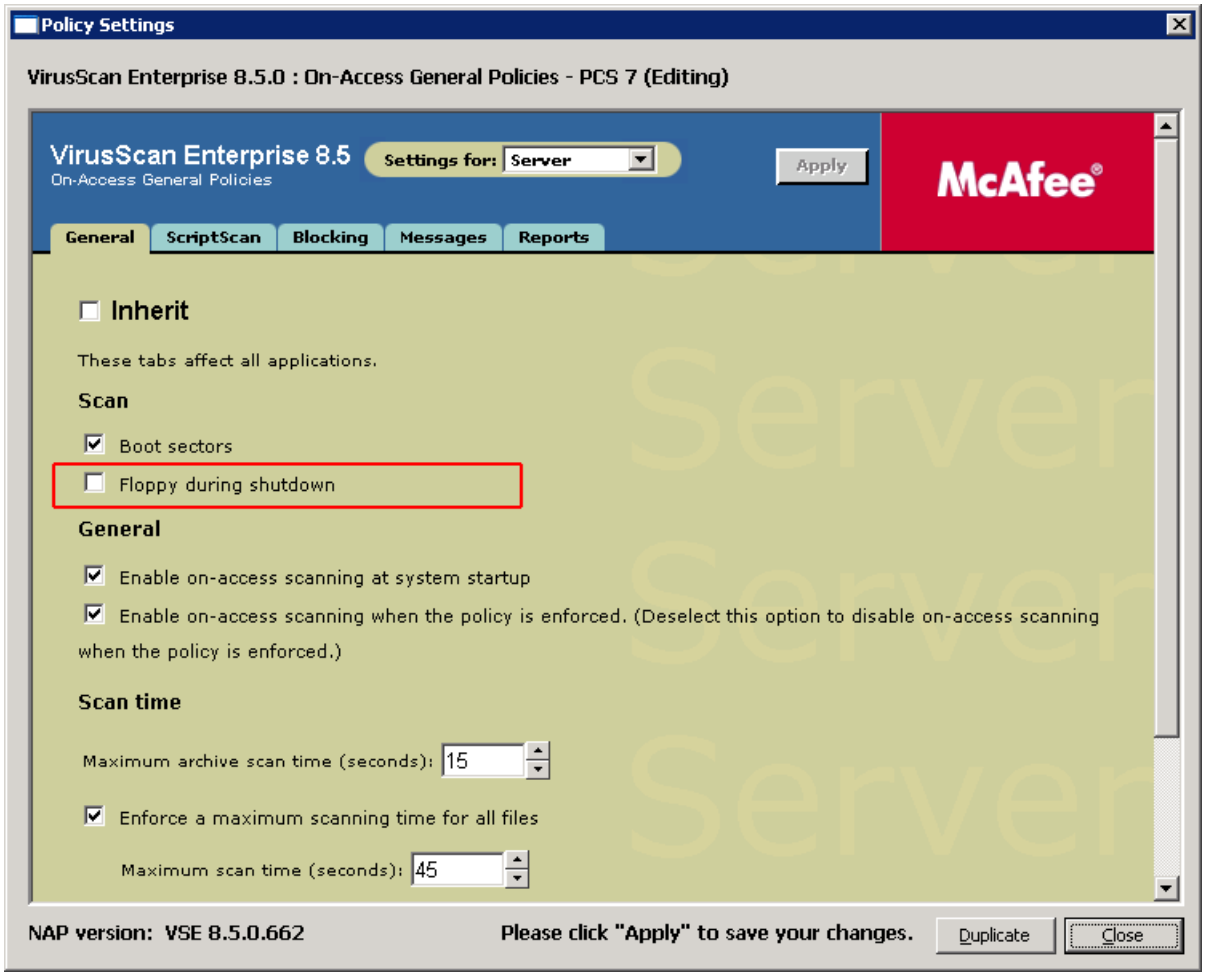


Figure 2-5 "On-Access General Policies" dialog box: "General" tab

2.4.2 "ScriptScan" tab

- Check box "Enable ScriptScan": **Enabled**

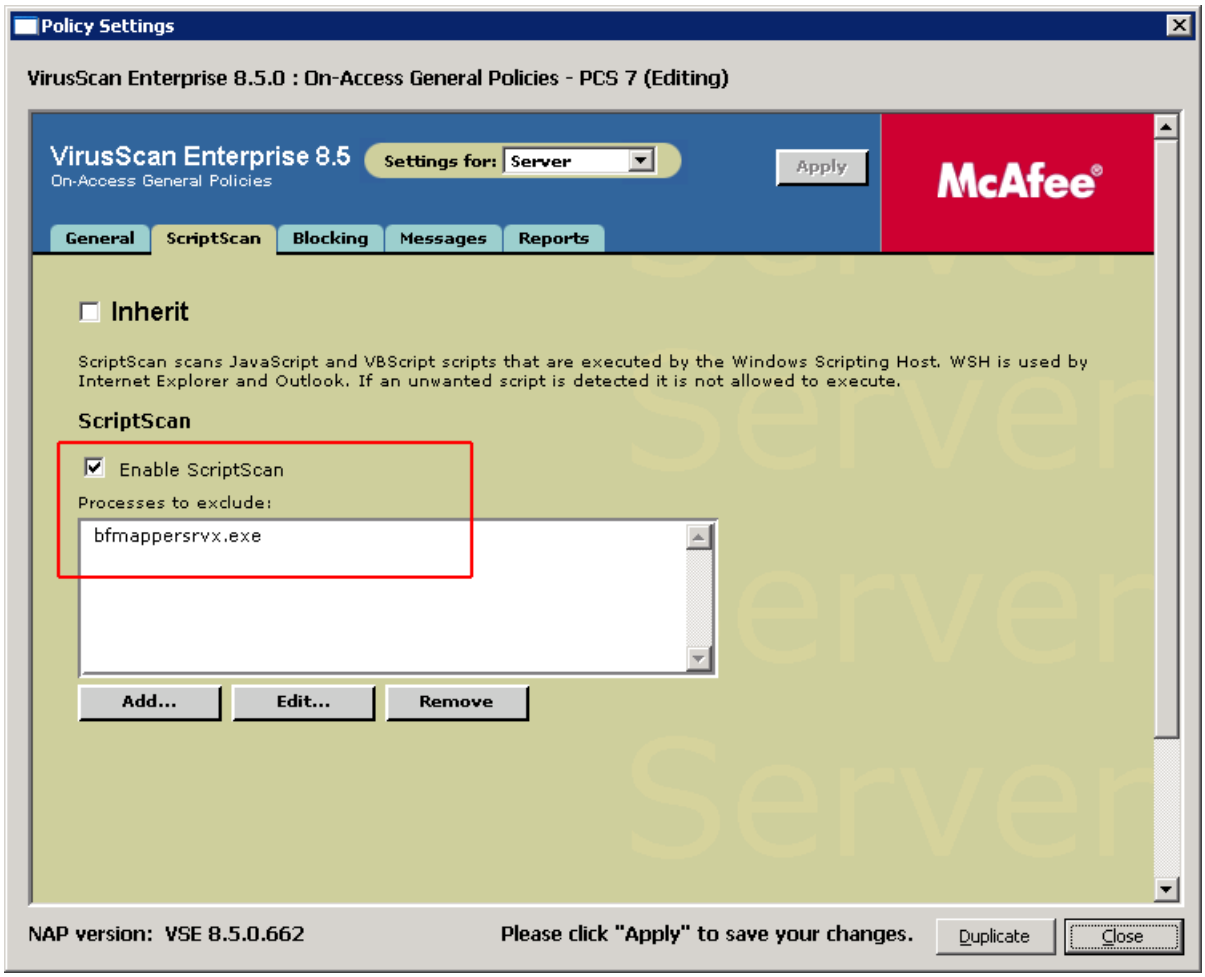


Figure 2-6 "On-Access General Policies" dialog box: "ScriptScan" tab

SIMATIC Batch Server / BATCH Single Station

On a SIMATIC BATCH server / BATCH single server, the application "bfmappersrvx.exe" must be entered in the "Excluded processes" field.

2.4.3 "Blocking" tab

- Check box "Block the connection": **Deactivated**

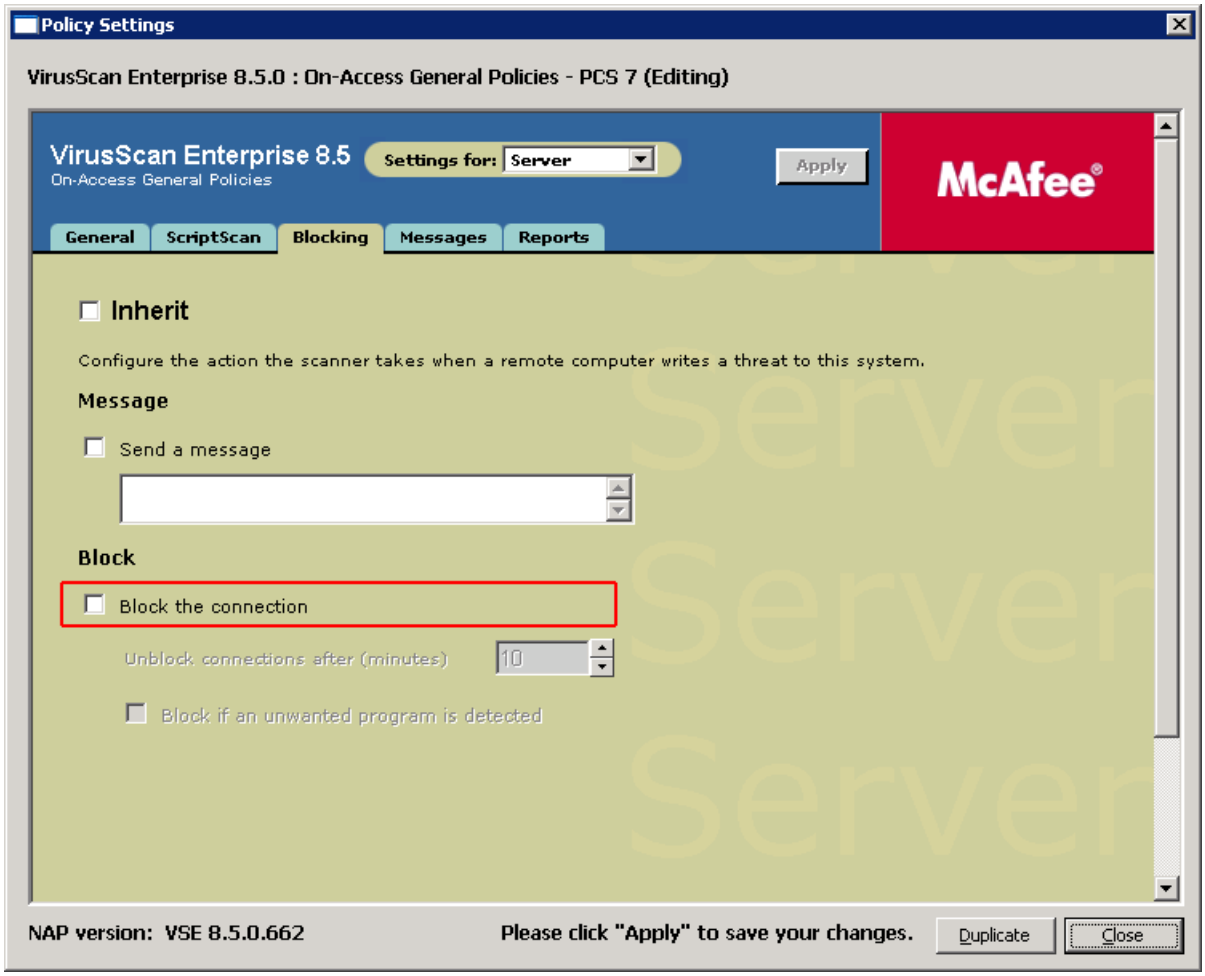


Figure 2-7 "On-Access General Policies" dialog box: "Blocking" tab

BATCH server / BATCH single station

On a BATCH server / BATCH single station, the application "bfmappersrvx.exe" must be entered in the "Excluded processes" field.

2.4.4 "Messages" tab

- Check box "Show the messages dialog when a detection occurs": **Disabled**
- Check box "Remove messages from the list": **Disabled**
- Check box "Clean files": **Disabled**
- Check box "Delete files": **Disabled**

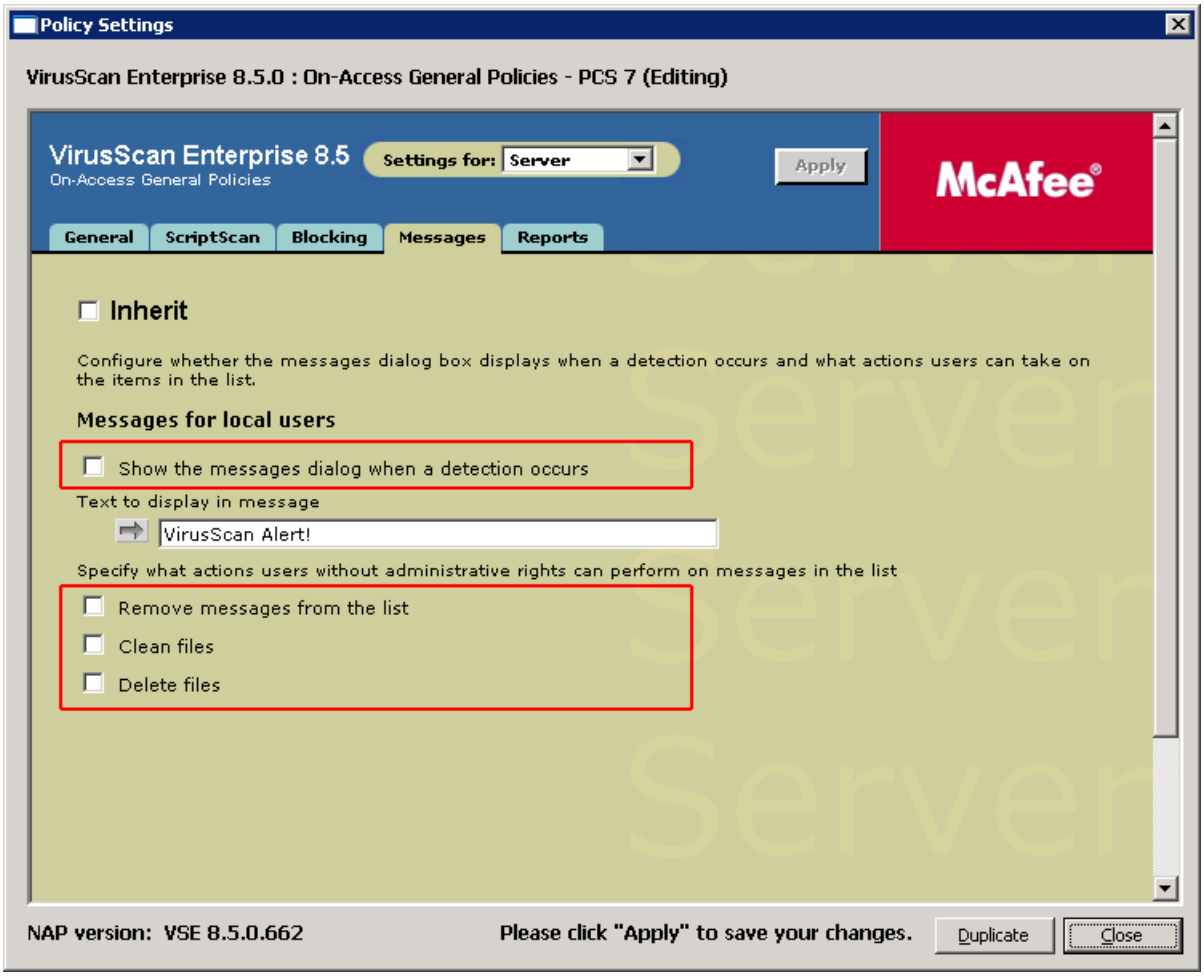

Policy Settings
VirusScan Enterprise 8.5.0 : On-Access General Policies - PCS 7 (Editing)
VirusScan Enterprise 8.5
On-Access General Policies
Settings for: Server
Apply
McAfee
General
ScriptScan
Blocking
Messages
Reports
Inherit
Configure whether the messages dialog box displays when a detection occurs and what actions users can take on the items in the list.
Messages for local users
Show the messages dialog when a detection occurs
Text to display in message
VirusScan Alert!
Specify what actions users without administrative rights can perform on messages in the list
Remove messages from the list
Clean files
Delete files
NAP version: VSE 8.5.0.662
Please click "Apply" to save your changes.
Duplicate
Close

Figure 2-8 "On-Access General Policies" dialog box: "Messages" tab

2.5 On-Access Default Processes Policies

2.5.1 "Detection" tab

- Check box "When reading from disk": **Disabled**
- Check box "On network drives": **Disabled**

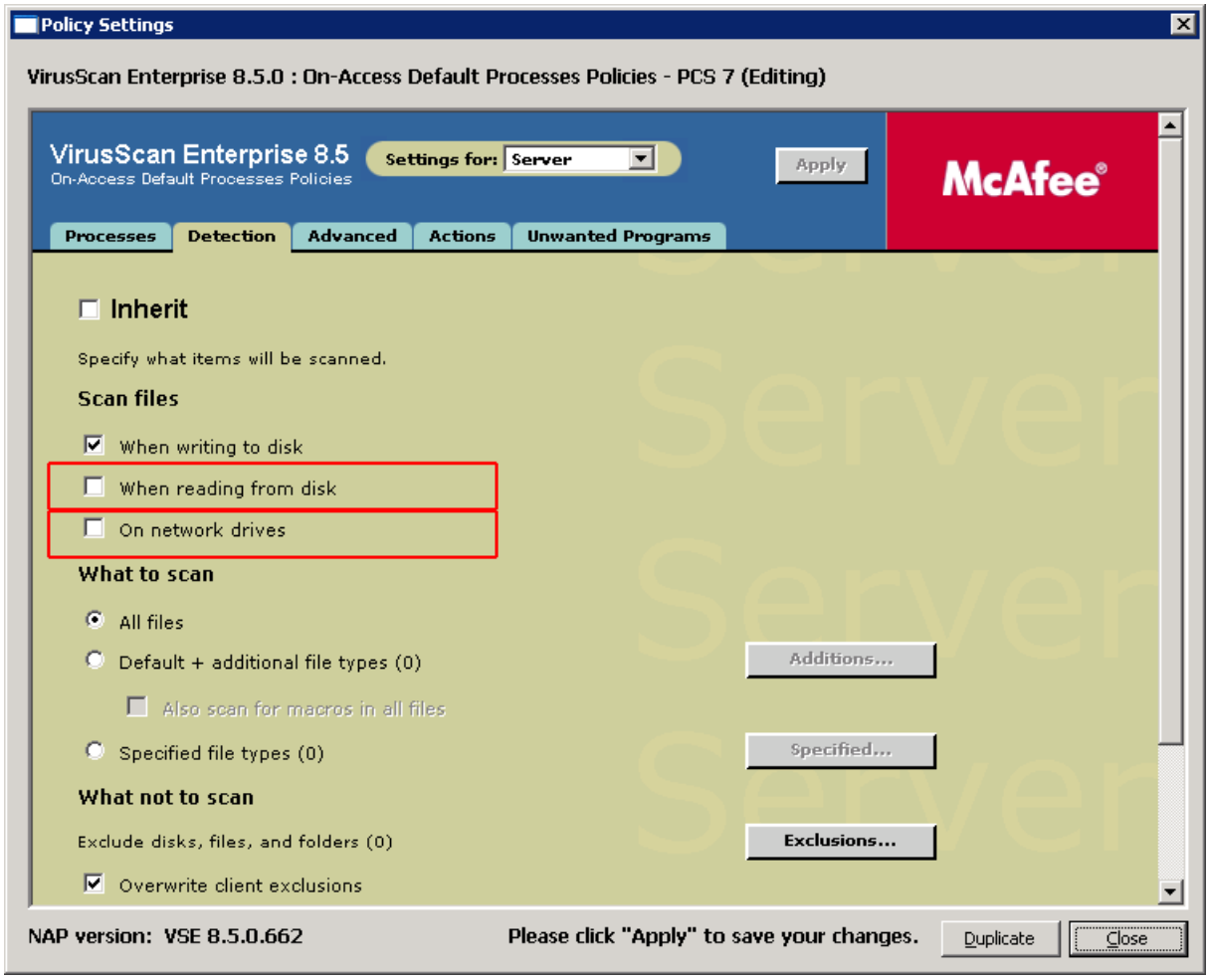


Figure 2-9 "On-Access Default Processes Policies" dialog box: "Detection" tab

2.5.2 "Advanced" tab

"Scan inside archives (e.g. ZIP)" check box: **Enabled**

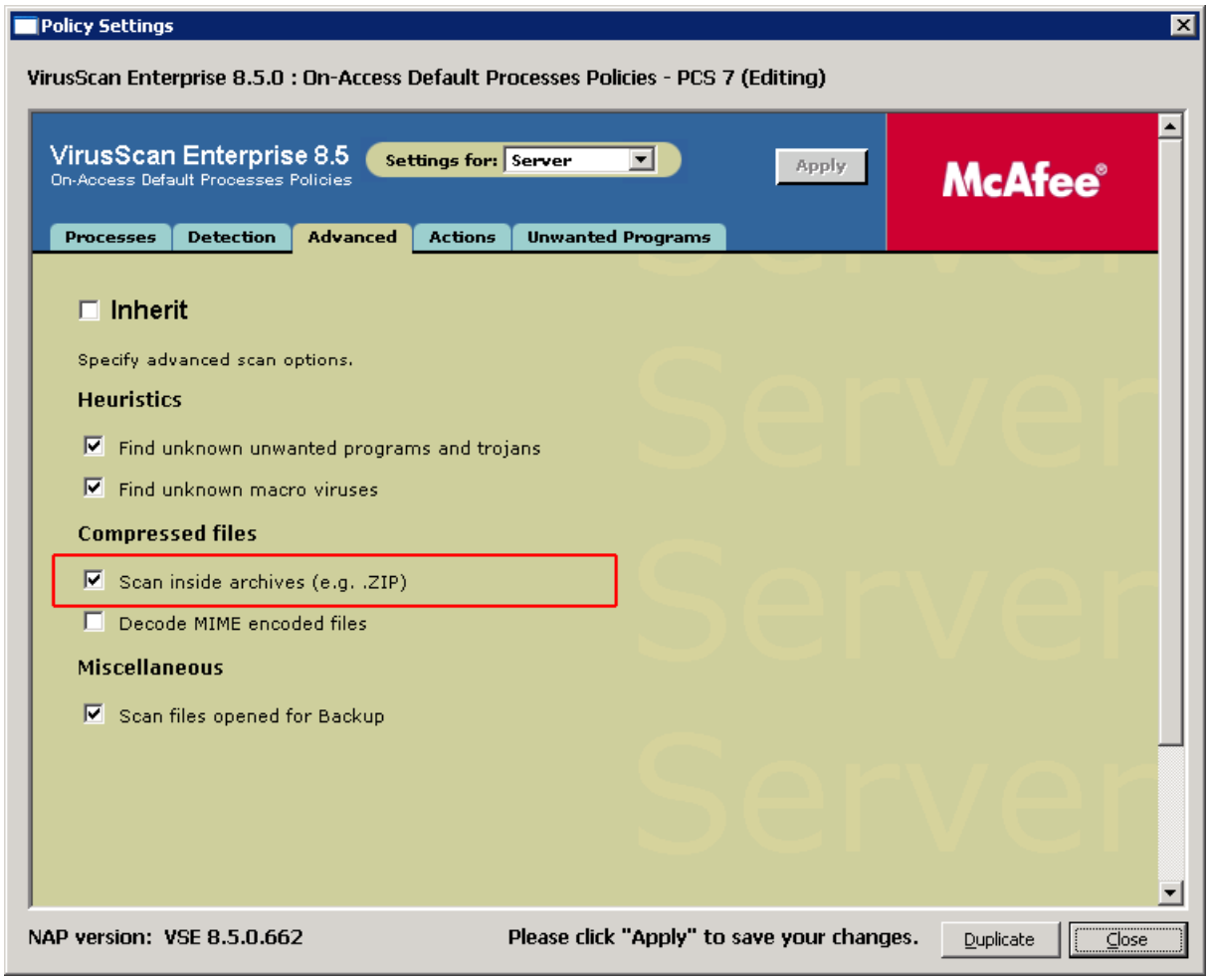


Figure 2-10 "On-Access Default Processes Policies" dialog box: "Advanced" tab

2.5.3 "Actions" tab

Important information

The following behavior is required in the PCS 7 security concept if a computer virus is found:

- After finding the virus: Alert message
- Then no further file operations without the intervention of the user

This should ensure that important project data is not destroyed.

This behavior cannot be configured in the McAfee VirusScan 8.5i.

- In the drop-down menu "Primary action - When a threat is found:" select "Clean files automatically".
- In the drop-down menu "Secondary action - When the first action fails:" select "Deny access to files".

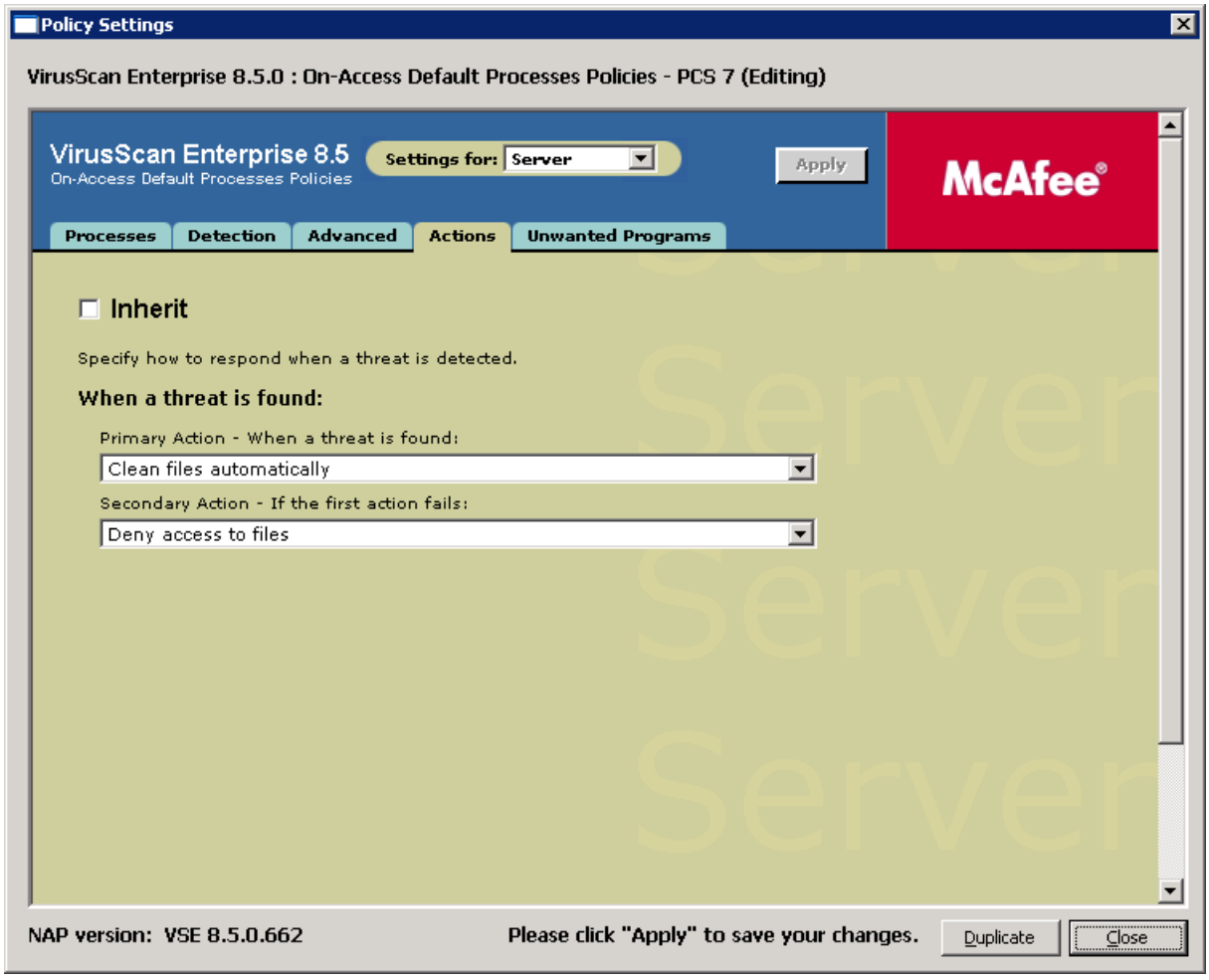


Figure 2-11 "On-Access Default Processes Policies" dialog box: "Actions" tab

2.5.4 "Unwanted Programs" tab

- In the drop-down menu "Primary action - When an unwanted program is found:" select "Allow access to the file".

Note

This should ensure that any software which has been incorrectly identified as an "unwanted program" is not restricted in its function.

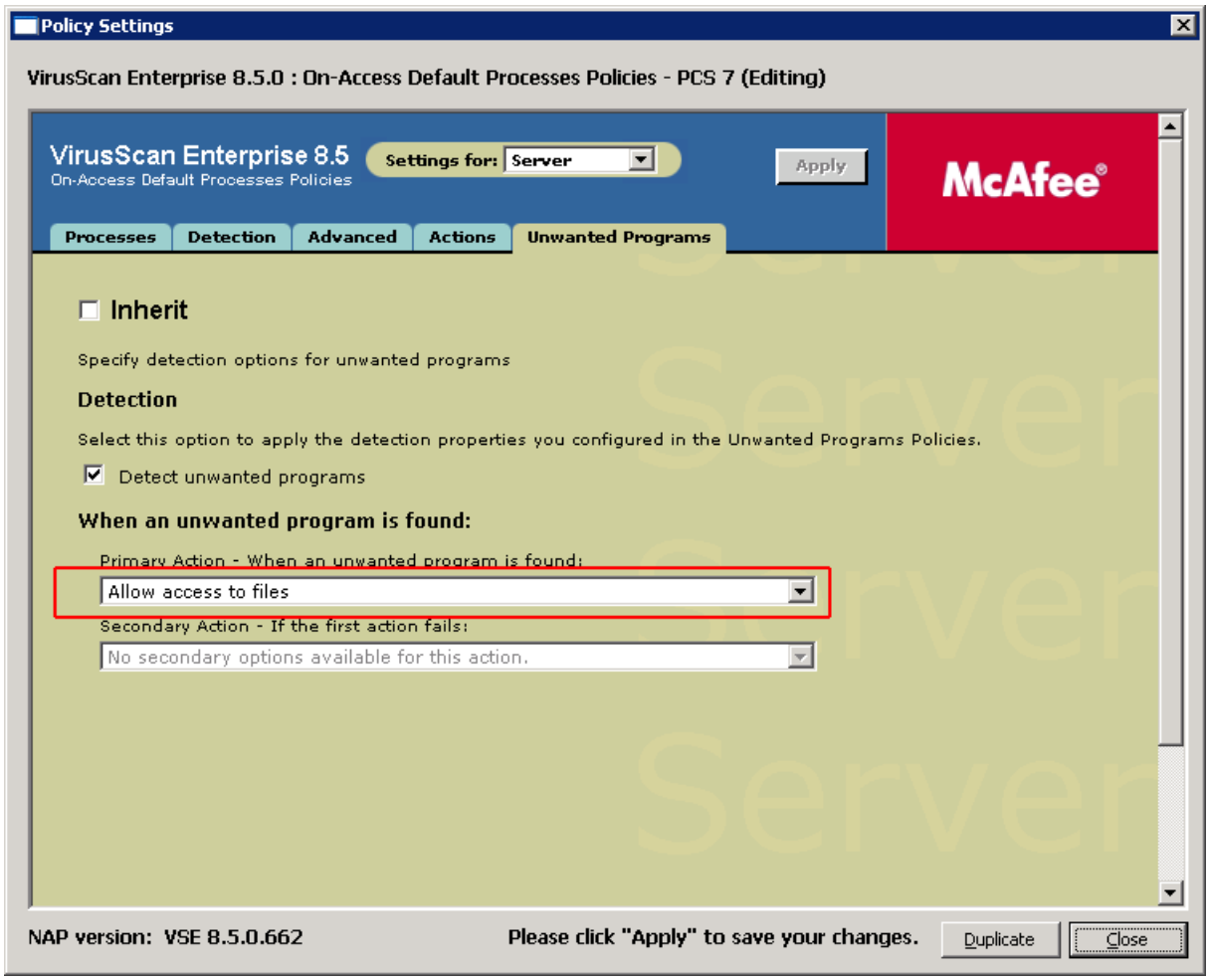

Policy Settings
VirusScan Enterprise 8.5.0 : On-Access Default Processes Policies - PCS 7 (Editing)
VirusScan Enterprise 8.5
On-Access Default Processes Policies
Settings for: Server
Apply
McAfee
Processes
Detection
Advanced
Actions
Unwanted Programs
Inherit
Specify detection options for unwanted programs
Detection
Select this option to apply the detection properties you configured in the Unwanted Programs Policies.
Detect unwanted programs
When an unwanted program is found:
Primary Action - When an unwanted program is found:
Allow access to files
Secondary Action - If the first action fails:
No secondary options available for this action.
NAP version: VSE 8.5.0.662
Please click "Apply" to save your changes.
Duplicate
Close

Figure 2-12 "On-Access Default Processes Policies" dialog box: "Unwanted Programs" tab

2.6 On-Access Low-Risk Processes Policies

Policy name: McAfee Default

These policies retain the McAfee default settings.

2.7 On-Access High-Risk Processes Policies

Policy name: McAfee Default

These policies retain the McAfee default settings.

2.8 On Delivery E-Mail Scan Policies Policies

Policy name: McAfee Default

These policies retain the McAfee default settings.

2.9 User Interface Policies

2.9.1 "Display Options" tab

- "Show the system tray with minimal menu options" radio button: **Enabled**
- "Enable splash screen" check box: **Disabled**

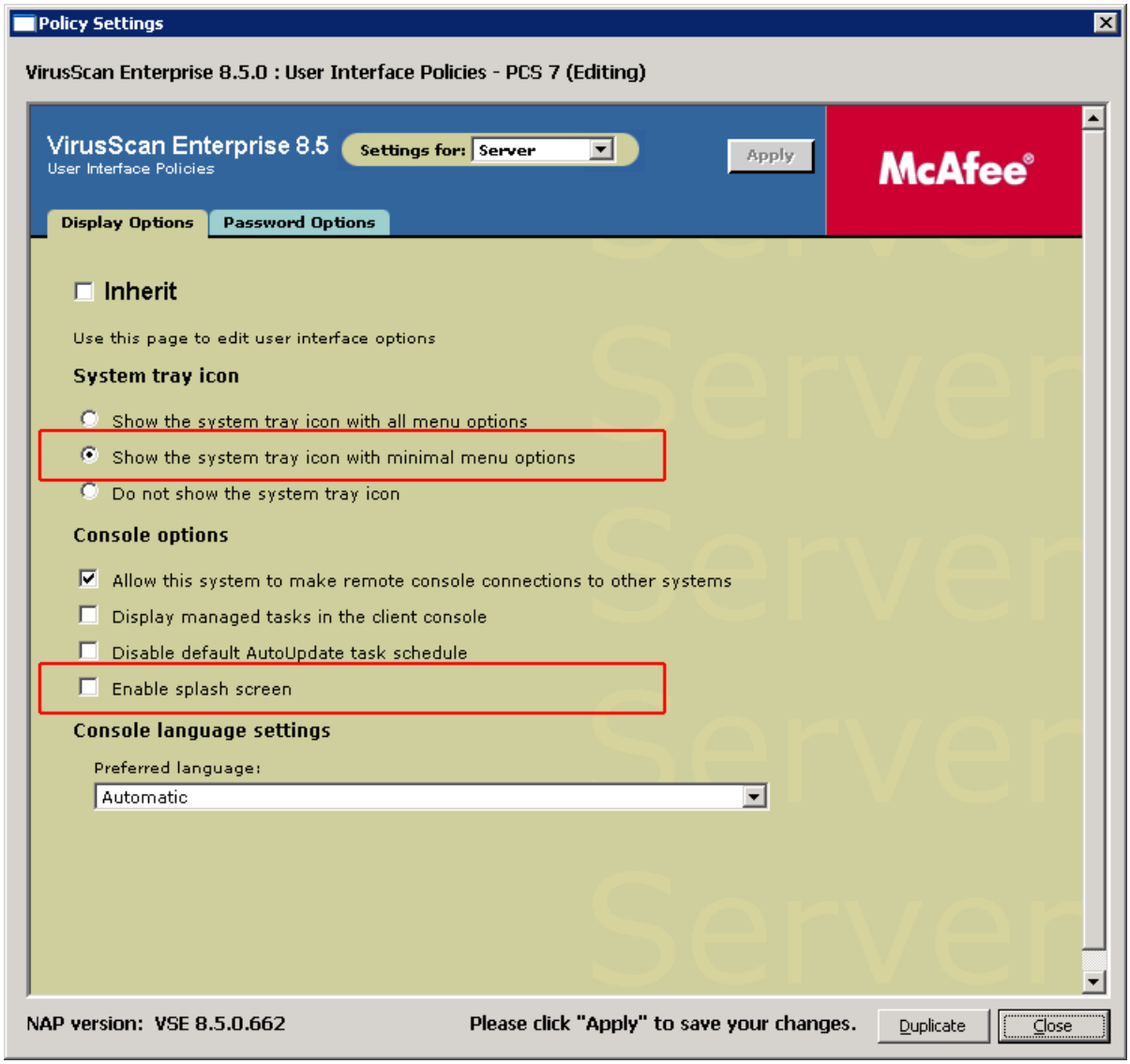

Policy Settings
VirusScan Enterprise 8.5.0 : User Interface Policies - PCS 7 (Editing)
VirusScan Enterprise 8.5
User Interface Policies
Settings for: Server
Apply
McAfee
Display Options
Password Options
Inherit
Use this page to edit user interface options
System tray icon
Show the system tray icon with all menu options
Show the system tray icon with minimal menu options
Do not show the system tray icon
Console options
Allow this system to make remote console connections to other systems
Display managed tasks in the client console
Disable default AutoUpdate task schedule
Enable splash screen
Console language settings
Preferred language:
Automatic
NAP version: VSE 8.5.0.662
Please click "Apply" to save your changes.
Duplicate
Close

Figure 2-13 "User Interface Policies" dialog box: "Display Options" tab

2.9.2 "Password Options" tab

- Option button "Password protection for all items listed:" **Enabled**

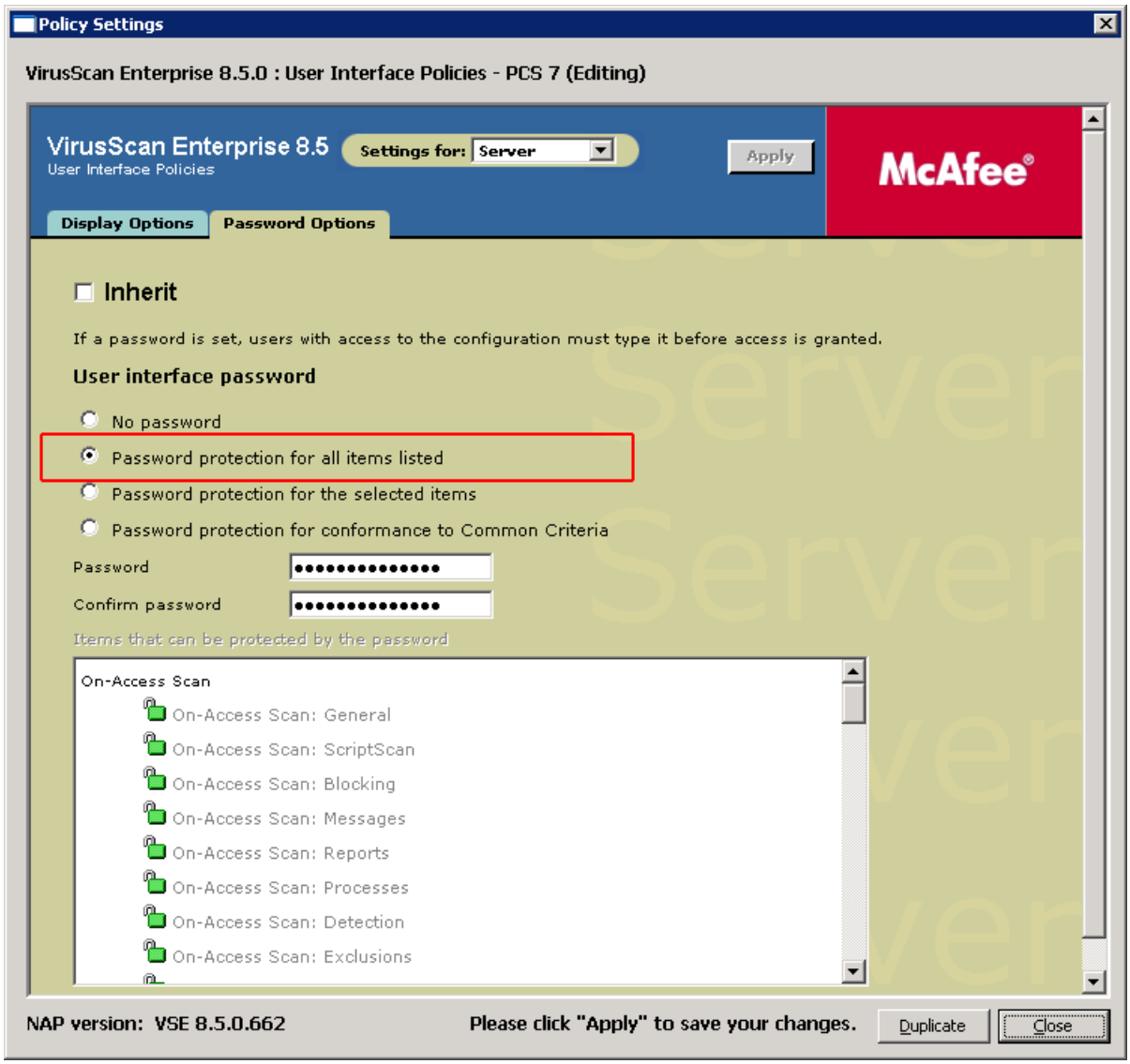


Figure 2-14 "User Interface Policies" dialog box: "Password Options" tab

2.10 Warning guidelines

Policy name: McAfee Default

These policies retain the McAfee default settings.

2.11 Access Protection Policies

Policy name: McAfee Default

These policies retain the McAfee default settings.

2.12 Buffer overflow protection policies

"Enable buffer overflow protection" check box: **Disabled**

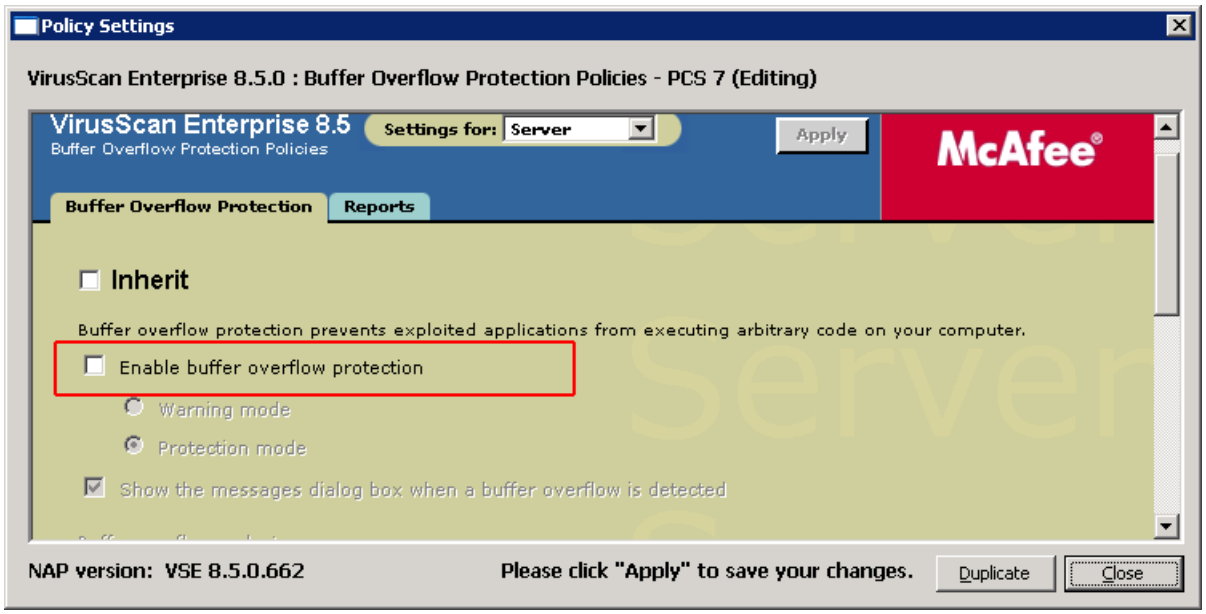

Policy Settings
VirusScan Enterprise 8.5.0 : Buffer Overflow Protection Policies - PCS 7 (Editing)
VirusScan Enterprise 8.5
Buffer Overflow Protection Policies
Settings for: Server
Apply
McAfee
Buffer Overflow Protection
Reports
Inherit
Buffer overflow protection prevents exploited applications from executing arbitrary code on your computer.
Enable buffer overflow protection
Warning mode
Protection mode
Show the messages dialog box when a buffer overflow is detected
NAP version: VSE 8.5.0.662
Please click "Apply" to save your changes.
Duplicate
Close

Figure 2-15 "Buffer Overflow Protection Policies" dialog box: "Buffer Overflow Protection" tab

2.13 Unwanted Programs Policies

Policy name: McAfee Default

These policies retain the McAfee default settings.

2.14 Quarantine Manager Policies

Policy name: McAfee Default

These policies retain the McAfee default settings.